REMARKS

The Examiner has rejected Claim 51 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The Examiner has specifically stated that applicant's claimed technique "wherein the heuristic rule includes information associated with an active networked application making a new connection never previously made" is not supported in the specification. Applicant respectfully points out page 5, lines 1-8 of the specification, which clearly states that "a heuristic rule may describe an attack that is based on unusual behavior, e.g. an application suddenly making a new, previously unseen connection" and that "[t]he system 100 applies a filter 103 based on the active networked applications." Thus, applicant's claim language is clearly supported by the specification.

The Examiner has rejected Claims 1-12, 14-26, 28-40, 42-48 and 50-51 under 35 U.S.C. 103(a) as being unpatentable over Freund (U.S. Patent No. 5,987,611) and in further view of Kaler et al. (U.S. Patent No. 6,671,829). Applicant respectfully disagrees with such rejection.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the first element of the *prima facie* case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner argues that it would have been obvious to combine the teaching of the subset of intrusion

rules in Freund with the teaching of filter reduction to extract only the information of interest as taught by Kaler because this reduces the performance impact of monitoring. To the contrary, applicant respectfully asserts that it would not have been obvious to combine the teachings of the Freund and Kaler references, especially in view of the vast evidence to the contrary.

For example, Freund relates to regulating access and maintaining security of individual computer systems and local area networks connected to larger open networks, while Kaler relates to analyzing the performance of a data processing system. To simply glean features from a security system, such as that of Freund, and combine the same with the *non-analogous art* of a performance analyzer, such as that of Kaler, would simply be improper. In particular, security systems actively protect computer systems, while performance analyzers merely collect data associated with a computer system for performance analysis. "In order to rely on a reference as a basis for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992) In view of the vastly different types of problems a security system addresses as opposed to a performance analyzer, the Examiner's proposed combination is inappropriate.

Applicant also respectfully asserts that the third element of the *prima facie* case of obviousness has also not been met by the references relied on by the Examiner. Specifically, with respect to each of the independent claims, the Examiner has relied on the following excerpts from Freund to make a prior art showing of applicant's claimed "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application" (see the same or similar, but not necessarily identical language in each of the independent claims).

"...the system can track files being created and changed by any process in order to match TCP/IP activities with corresponding file activities." (Col. 4, lines 65-67)

"...which specifies rules which govern Internet access by the client computers including the particular client computer;
c) Transmitting a filtered subset of the rules to the particular client computer." (Col. 5, lines 39-43)

Applicant respectfully asserts that the only rules in such excerpts relate to "rules which govern Internet access by the client computers." Clearly, rules that govern Internet access do not meet applicant's claimed "rules corresponding to the active networked application" (emphasis added).

Furthermore, simply because Freund teaches that a "system can track files created and changed by any process" does not inherently mean that there are rules corresponding to an active networked application, in the manner claimed by applicant.

Still yet, such excerpts do not even mention any sort of filtering, let alone "filtering a set of intrusion rules to create a subset of intrusion rules," as applicant specifically claims (emphasis added). In fact, applicant notes that the only subset of rules disclosed in Freund relate to "rules filtered for a given user" (see Claim 12 in Freund), and not to applicant's claimed "subset of intrusion rules corresponding to the active networked application" (emphasis added).

In addition, with respect to each of the independent claims, the Examiner has relied on the following excerpts from Freund to make a prior art showing of applicant's claimed technique "where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application" (see the same or similar, but not necessarily identical language in each of the independent claims).

"e) Determining whether the request for Internet access would violate any of the rules transmitted to the particular client computer, and
f) If the request for Internet access violates any of the rules transmitted to the particular client computer, denying the

request for Internet access.
II. Using Application Properties to Determine Legitimate Internet Traffic
a) Application attempts to access Internet;
b) Client Monitor compares application properties (version, executable name, and the like) with database of application allowed to access the Internet and checks what kind of activity the application is allowed to do (mail, browsing, and the like)." (Col. 5, lines 46-59-emphasis added)

"(1) The system should preferably be capable of restricting access to the Internet (or other Wide Area Network) to certain approved applications or/and application versions.
(2) The system should preferably support centrally-maintained access rules (e.g., defining basic access rights), but at the same time allow individual workgroup managers or even individual users to set rules for their area of responsibility, if so desired by the organization." (Col. 8, lines 45-52)

Applicant respectfully asserts that such excerpts only relate to accessing the Internet, including rules associated with applications that are allowed to access the Internet (see emphasized excerpt above). Clearly, only teaching rules regarding accessing the Internet does not meet applicant's specific claim language, namely a "subset of the intrusion rules corresponding to the active networked application [that] are capable of being used for evaluating intrusions that target the corresponding **active networked application**" (emphasis added).

Still yet, with respect to each of the independent claims, the Examiner has relied on the following excerpts et al. from Freund and Kaler to make a prior art showing of applicant's claimed technique "wherein the subset of the intrusion rules corresponding to the active networked application are used for the evaluation for reducing a required amount of processing resources."

"If a process uses FTP to download a file, for example, the system will match that activity to a file being saved by the same process by checking file name and size. If a match is found, a log entry is generated. This allows the immediate application of internal or external virus checkers." (Freund: Col. 13, lines 59-65)

"Filter reduction is used to narrow the scope of the filter to extract only the information of interest and hence reduce the performance impact of monitoring." (Kaler: Col. 4, lines 57-61)

First, applicant respectfully asserts that the excerpt in Freund relied on by the Examiner does not even suggest any sort of "subset of the intrusion rules," as the Examiner contends (emphasis added), but instead only teaches matching activity to a file. Thus, since Freund does not disclose a subset in the context claimed by applicant, Freund cannot teach, even in combination with Kaler, a subset that is "used for the evaluation for reducing a required amount of processing resources." Furthermore, applicant notes that, when read in context, Kaler's filter reduction only relates to a user that specifies which items to filter such that events are collected only for the specified items (see Kaler, Col. 37, line 47- Col. 38, line 5). Thus, Kaler does not teach a subset of intrusion rules, as claimed by applicant, but instead only teaches a filter which collects events for specified items.

Since at least the first and third elements of the *prima facie* case of obviousness has not been met, as noted above, a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. Just by way of example, with respect to Claim 2 et al., the Examiner has relied on Col. 4, lines 51-62 in Freund to make a prior art showing of applicant's claimed "detecting when the active networked application becomes inactive; and re-filtering the set of intrusion rules." Applicant respectfully asserts that the only mention of an application in such excerpt merely relates to a "system [that] can monitor TCP/IP activities on a...per application basis." Freund simply fails to even suggest a situation where an "active networked application becomes inactive" (emphasis added), and especially does not teach that, when such occurs, "the set of intrusion rules [are re-filtered]," as claimed by applicant.

With respect to Claims 3 and 4 et al., the Examiner has relied on Col. 13, lines 20-22 in Freund to make a prior art showing of applicant's claimed technique "wherein the detecting comprises: monitoring network connection terminations" (Claim 3 et al.)

and "wherein the detecting comprises: monitoring application terminations" (Claim 4 et al.). Applicant respectfully asserts that such excerpt from Freund only discloses that "if a rule is violated...[then] Internet access [is denied]." Clearly, denying internet access in the case that a rule is violated does not even suggest any sort of monitoring, let alone specifically "monitoring network connection terminations" and/or "monitoring application terminations," as claimed by applicant.

With respect to Claim 5 et al., the Examiner has relied on Col. 13, lines 50-56 and Col. 26, lines 55-58 in Freund to make a prior art showing of applicant's claimed "detecting when no networked application is active; and suspending the evaluating of network traffic until a networked application is active." Applicant respectfully asserts that such excerpts only relate to "prescribed remedial action for any violated rule" such that "the communication is...terminated." Clearly, terminating a communication upon detection of a rule violation, as in Freud, does not even remotely relate to applicant's claim language, namely "detecting when no networked application is active," let alone where "the evaluating of network traffic [is suspended] until a networked application is active" (emphasis added).

With respect to Claim 6 et al., the Examiner has again relied on Col. 13, lines 50-56 and Col. 26, lines 55-58 in Freund to make a prior art showing of applicant's claimed "continuing the evaluating of network traffic if no networked application is active." Applicant respectfully asserts that such claim language is not met by the Freund references for substantially the same reasons as argued above with respect to Claim 5 et al.

With respect to Claim 48, the Examiner has relied on Col. 11, line 56-Col. 12, line 17 and Col. 13, lines 13-22 in Freund to make a prior art showing of applicant's claimed technique "wherein the intrusion rules include information selected from the group consisting of a targeted active networked application, a specific hostile payload, a network port, and a protocol." Applicant respectfully asserts that Col. 11, line 56-Col. 12, line 17 does not relate to intrusion rules, as claimed by applicant, but instead only

relates to the protocol the Internet uses. In addition, Col. 13, lines 13-22 only discloses that the rules can specify "to whom the rule should apply...start date and expiration date of a rule; time of day when the rules should be applied...whether the rule is 'disclosed' to the user or workgroup...whether a rule ca be overwritten...and what should happen if a rule is violated." Clearly, such information associated with the rules as taught in Freund only relate to the application of the rules, and not to the substance of the rules including "a targeted active networked application, a specific hostile payload, a network port, and a protocol," as specifically claimed by applicant.

With respect to Claim 51, the Examiner has relied on Col. 10, lines 31-44; Col. 30, lines 13-15; Col. 13, lines 34-42; and Col. 5, lines 39-43 in Freund to make a prior art showing of applicant's claimed technique "wherein the heuristic rule includes information associated with an active networked application making a new connection never previously made." Applicant respectfully asserts that such excerpts only disclose that a "given application itself can be examined for determining whether it is 'active' by determining whether the application receives 'focus' and/or receives user input," "maintain[ing] a list of active Applications," "each client process can be checked for various characteristics," and "rules which govern Internet access." First, applicant respectfully asserts that such excerpts do not even suggest any sort of heuristic rule, as claimed by applicant. Second, only determining which applications are actively used by a user, as in Freund, clearly does not meet any sort of "information associated with an active networked application making a new connection never previously made," as specifically claimed by applicant (emphasis added).

Again, since at least the first and third elements of the *prima facie* case of obviousness has not been met, as noted above, a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P345/01.239.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100